

ABM PARKING SERVICES INC. PROVIDES PUBLIC NOTICE OF VENDOR'S DATA SECURITY INCIDENT AT NINE CHICAGO PARKING LOTS

CHICAGO, IL – December 5, 2014 – ABM Parking Services, Inc. (“the company”), today announced that Datapark USA Inc. a vendor that provides and maintains point of service software for several Chicago, Illinois parking facilities managed by the company, has confirmed a data security incident. This incident may involve certain customer credit and debit card information, including payment card numbers.

After being notified by Datapark of a potential compromise, the company launched an investigation to: confirm the nature of any unauthorized access to its system; identify any information that may have been exposed; and quickly remediate the compromise. The company engaged independent data forensic experts to assist with the investigation. At this time, the company believes the following Chicago locations were affected during the indicated dates:

- 130 E. Randolph St., Chicago, IL 60601 (9/29/14 – 10/29/14)
- 1 South Wacker Dr., Chicago, IL 60606 (9/30/14 – 10/30/14)
- 225 W. Wacker Dr., Chicago, IL 60606 (9/29/14 – 10/31/14)
- 303 E. Wacker Dr., Chicago, IL 60601 (9/29/14 – 10/29/14)
- 55 East Jackson Blvd., Chicago, IL 60604 (9/30/14 – 10/29/14)
- 60 E. Randolph St., Chicago, IL. 60601 (10/6/14 – 10/31/14)
- 227 W. Monroe St., Chicago, IL 60606 (9/30/14 – 11/18/14)
- 10-30 South Wacker Dr., Chicago, IL 60606 (9/29/14 – 11/3/14)
- 111 E. Wacker Dr., Chicago, IL 60601 (9/29/14 – 11/1/14)

The company encourages customers who used payment cards (i.e., credit or debit cards) for transactions on the dates noted at these locations to review their payment card statements for signs of unusual activity. Datapark has indicated that it has “blocked access to prevent any further unauthorized entry into the[ir] servers.” The forensic evidence indicates that the compromise was limited to payment card data and that no other personally identifiable information was exposed. Law enforcement and the credit card brands have been notified of this incident.

A toll-free information line is available for customers at (877) 238-3790. To help protect your identity and credit card information, ABM is offering all affected individuals a **complimentary** one-year membership of Experian’s® ProtectMyID® Elite. This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft. You may enroll by calling (877) 238-3790.

The company encourages customers to remain vigilant and seek to protect against possible misuse of credit cards, identity theft, or other financial loss by reviewing account statements for any unusual activity, notifying their credit card companies, and monitoring their credit reports. Under U.S. law, individuals are entitled to one free credit report annually from each of the three major credit bureaus. To obtain a free credit report, visit <http://www.annualcreditreport.com/> or call, toll-free, (877) 322-8228.

At no charge, customers can also have these credit bureaus place a "fraud alert" on their files that alerts creditors to take additional steps to verify their identity prior to granting credit in their names. Please note, however, that because it tells creditors to follow certain procedures to protect the individual's credit, a fraud alert may also delay the ability to obtain credit while the agency verifies the individual's identity. As soon as one credit bureau confirms an individual's fraud alert, the others are notified to place fraud alerts on that individual's file. Any individual wishing to place a fraud alert, or who has questions regarding their credit report, can contact any one of the following agencies: Equifax, P.O. Box 105069, Atlanta, GA 30348-5069, 800-525-6285, www.equifax.com; Experian, P.O. Box 2002, Allen, TX 75013, 888-397-3742, www.experian.com; or TransUnion, P.O. Box 2000, Chester, PA 19022-2000, 800-680-7289, www.transunion.com. Information regarding security freezes may also be obtained from these sources.

The Federal Trade Commission (FTC) also encourages those who discover that their information has been misused to file a complaint with them. To file a complaint with the FTC, or to obtain additional information on identity theft and the steps that can be taken to avoid identity theft, the FTC can be reached at 600 Pennsylvania Avenue NW, Washington, D.C. 20580, or at www.ftc.gov/bcp/edu/microsites/idtheft/ or (877) ID-THEFT (877-438-4338); TTY: (866) 653-4261. State Attorneys General may also have advice on preventing identity theft, and instances of known or suspected identity theft should be reported to law enforcement, the Attorney General in the individual's state of residence, and the FTC. Individuals can also learn more about placing a fraud alert or security freeze on their credit files by contacting the FTC or their state's Attorney General. For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, (919) 716-6400, www.ncdoj.gov. For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, (888) 743-0023, <http://www.oag.state.md.us>.

ABM PARKING SERVICES INC. PROVIDES PUBLIC NOTICE OF VENDOR'S DATA SECURITY INCIDENT AT NINE CHICAGO PARKING LOTS

ABM Parking Services, Inc. ("the company") announced that Datapark USA Inc., a vendor which provides and maintains point of service software for several Chicago, Illinois parking facilities operated by the company, has confirmed a data security incident that affects personal information of certain parking lot customers. The company is issuing this public notice and encouraging individuals who used payment cards (i.e., credit or debit cards) for transactions from late September 2014 through mid-November 2014 at Chicago parking facilities to review their payment card statements for signs of unusual activity and to take steps to protect their identities and financial information. A toll-free, confidential information line is available to customers at (877) 238-3790.

Under Massachusetts law, you have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

Massachusetts law gives you the right to place a security freeze on your consumer reports. A security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. Using a security freeze, however, may delay your ability to obtain credit. You may request that a freeze be placed on your credit report by sending a request to a credit reporting agency by certified mail, overnight mail, or regular stamped mail to the address below:

Equifax, P.O. Box 105788, Atlanta, GA 30348, www.equifax.com

Experian, P.O. Box 9554, Allen, TX 75013, www.experian.com

TransUnion, P.O. Box 2000, Chester, PA 19022, www.transunion.com

Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. The following information should be included when requesting a security freeze (documentation for you and your spouse must be submitted when freezing a spouse's credit report): full name, with middle initial and any suffixes; Social Security number; date of birth (month, day and year); current address and previous addresses for the past five (5) years; and applicable fee (if any) or incident report or complaint with a law enforcement agency or the Department of Motor Vehicles. The request should also include a copy of a government-issued identification card, such as a driver's license, state, or military ID card, and a copy of a utility bill, bank, or insurance statement. Each copy should be legible, display your name and current mailing address, and reference the date of issue (statement dates must be recent). The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both, that can be used by you to authorize the removal or lifting of the security freeze. The credit reporting company may charge a reasonable fee of up to \$5 to place a freeze or lift or remove a freeze, unless you are a victim of identity theft or the spouse of a victim of identity theft, and have submitted a valid police report relating to the identity theft to the credit reporting company.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time. To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.